Robo de IDentidad MX

REVISTA DIGITAL

Número 2

Artículos:
La IDentidad y los pueblos indígenas.

El ABC del Artículo 71

PRO Tips:
Cómo proteger tu IDentidad.
6 tips fáciles de seguir.

Infografía:
Los niños y la seguridad en Internet.

Banco de conocimientos:
Los datos biométricos (2a. parte).

El Robo de IDentidad desde la visión de

GUEORGUI NIKOLOV POPOV

"Hay dos formas de vender cosas en este mundo; una es la felicidad, y la otra es con miedo, con terror, con pánico. Desafortunadamente, el tema de la identidad cae más en el pánico"

Entrevista con el Director General del FIMPE

Artículo:
Account Takeover. Qué es y cómo prevenirlo.

Artículo:
Cómo cuidar la IDentidad de los niños.

Infografía:
¿Qué es el Doxing y cómo evitarlo.

Y mucho más...

Robo de IDentidad MX
REVISTA DIGITAL

CONTENIDO:

Comité Editorial:

Iván Rodríguez - Director General

Luz González - Redacción

Arturo Douglas - Diseño

Colaboran en este número:

José Cadena
Adrián Cervantes Jaime
Vanessa Martínez Mandujano
Héctor Ortega

Revista Digital Robo de Identidad MX
Heriberto Frías 1145, Col. del Valle Centro,
03100, Ciudad de México.
Teléfonos: (55) 9191-6788 y (55) 5434-4438
Email: revista@robodeidentidad.mx
Website: robodeidentidad.mx

BIENVENIDOS

Nos encontramos transitando en un mundo donde la digitalización nos ha facilitado el acceso a servicios, nos ha ayudado a simplificar trámites y otras muchas bondades que nos ahorran tiempo y recursos.

En cada etapa de la vida del ser humano contemporáneo, el contacto con la tecnología en la cotidianeidad es cada vez mayor, ya que incluso los más pequeños se encuentran expuestos a pantallas con las que comparten información que no imaginamos, y que no compartiríamos con cualquiera.

Sin embargo, estas nuevas posibilidades de simplificar nuestras vidas, también nos hacen más vulnerables a nuevos delitos como el robo de identidad. En este sentido ¿nos hemos preguntado qué riesgos corre nuestra identidad en este contexto?

Lamentablemente, las cifras nos indican lo contrario. En nuestro país, las cifras de robo de identidad han aumentado de manera considerable en los últimos años, trayendo consigo pérdidas económicas y vulnerando a gran número de ciudadanos.

Pero, en concreto, ¿qué podemos hacer ante esto? Sin lugar a dudas, estar preparados, y la mejor manera de estarlo es sabiendo dónde nos encontramos, conociendo a detalle la magnitud de la situación internacional y local para permitirnos tomar medidas que nos brinden la seguridad necesaria a nosotros y a nuestros seres queridos. Además, educar a los más vulnerables para que crezcan con la menor fragilidad posible y con consciencia de los riesgos que corren y cómo pueden evitarlos.

En esta publicación compartimos artículos que buscan dar respuesta a las preguntas planteadas en este texto, con la finalidad principal de poner en la agenda una conversación acerca de las implicaciones del robo y suplantación de identidad, además de plantear una reflexión acerca de cómo la identidad digital puede jugar un rol fundamental en alcanzar las metas del desarrollo sustentable. A nivel global, puede permitir que la población más vulnerable y con menores recursos tenga acceso a servicios fundamentales desde la educación hasta los servicios de salud y financieros, mientras se avanza en sus derechos legales y políticos.

Iván Rodríguez | Director General RIDMX

"CONTROLA EL ROBO DE IDENTIDAD Y DISFRUTA LA VIDA"

Iván Rodríguez

ENTREVISTA CON: GUEORGUI NIKOLOV POPOV

Por: RIDMX

Gueorgui Nikolov Popov, es uno de nuestros especialistas invitados en el gran ecosistema que es la **Revista Robo de Identidad MX**. Egresado de la **Universidad Iberoamericana**, es **Director general y coordinador ejecutivo del Fideicomiso para Extender a la Sociedad los Beneficios del Acceso a la Infraestructura de los Medios de Pago Electrónicos (FIMPE)**, colabora con el **Banco Mundial** en la iniciativa global de inclusión financiera **"FiGi"**, ha sido ponente en diversos foros nacionales e internacionales relacionados con inclusión financiera, identidad, seguridad, transporte y tecnología. Ejecutivo experimentado con una amplia trayectoria de trabajo en la industria bancaria y financiera. Especializado en soluciones de identidad, sistemas de pago de transporte, programas de lealtad, tarjetas de pago, cajeros automáticos, pagos electrónicos y sistemas de punto de venta (POS).

Revista robo de identidad MX (RIDMX): ¿Cuál es la situación en el país del Robo de Identidad en menores, niños, niñas y adolescentes **(NNA)**?

Gueorgui Nikolov Popov (GNP): En México contamos con el **INE** que es nuestra credencial para votar, la credencial de identidad pero sólo sirve en este país, si vas a otro lado del mundo no sirve de mucho pues no es aceptada para validar que eres "tu", para rentar un automóvil, entrar a un hotel, etc.

Si hablamos de robo de identidad de niños, es importante hablar también de la trata de menores y robo de estos **NNA**. Es un tema delicado e importante pues en México se deberían establecer ciertas regulaciones para las personas que salen del país acompañados de **NNA**. Crear la solución, que no existe hoy en día, para que ambos padres autoricen biométricamente o con alguna identidad digital, la salida de los niños del país, en dado caso de que vaya uno o ambos padres o no vaya acompañado el menor.

Ahora bien, bajo los lineamientos de **Robo de Identidad a los menores**, si se comete fraude o cualquier delito, creo que es más probable que culpen de responsabilidad al tutor, al menos hasta que cumpla los dieciocho años. Quizá en esos momentos no se vea reflejado algún problema, por ello se debería emplear la tecnología existente para generar una Identidad digital en los niños y que en este lapso de tiempo (en lo que llegan a la mayoría de edad) no sufran ningún delito de esta índole

(RIDMX): ¿Qué tan grave puede ser que dicho delito le ocurra a los **NNA**?

(GNP): La gravedad en este asunto es más bien: ¿qué tanto puedes afectar en el futuro de los **NNA**? No me preocupa tanto el presente, más bien habrá que valorar las implicaciones que tiene legalmente, pero veo más riesgo en su futuro, es decir cuando cumpla la mayoría de edad.

(RIDMX): ¿Cuál cree que es la situación actual en México, en temas de **Seguridad y Robo de Identidad**?

(GNP): Tenemos una situación derivada por la falta de toma de decisiones, el **Robo de Identidad** se pudo haber mitigado hace mucho tiempo, desde que existe la tecnología para poderlo hacer, pero este tipo de cosas ocurren en todos los países. Y es un escenario muy grave, podemos ver casos en la compra y venta de coches, en la venta de inmuebles, en la contratación de seguros, en las casas de empeño, lo que conlleva a otro tipo de fraudes: lavado de dinero, extorsión. ¿Cuántos casos hemos escuchado de las llamadas para pedir dinero?

Los únicos que han trabajado arduamente para combatir dicho delito, que últimamente se ha vuelto más común, son los de las **AFORES**. Hace poco los mismos promotores hacían los cambios de **AFORE**, primero les pedían que se tomaran una foto para corroborar que era el usuario quien había solicitado el cambio, como notaron que no era suficiente, implementaron otras medidas de seguridad: que se tomaran una "selfie" junto con el promotor, pero de igual manera no resultó. Finalmente optaron por la toma de huellas dactilares, lo que logro que hoy en día no haya fraudes en los cambios de **AFORES**. Este es un caso en el que realmente se está empleando de manera benéfica el uso de la biometría.

"SIEMPRE HE DICHO QUE TENEMOS QUE HACER ALGO PORQUE, DE LO CONTRARIO, TODOS NOS VOLVEMOS CÓMPLICES DE TODO LO QUE ESTÁ OCURRIENDO EN EL PAÍS."

Gueorgui Nikolov Popov

También existen los casos de los Programas Sociales que en estos últimos 10 años se han entregado cerca de **380 mil millones de pesos** y realizado **515 millones de autenticaciones biométricas**; para el uso social, ha sido el caso más utilizado de una identidad digital creada con tecnología biométrica. A pesar de que nos hemos encontrado con muchas personas que no hablan el español, tienen claro que cuando se les genera una identidad digital, que no se puede violar, que gracias a ella sólo el titular puede recibir el apoyo, se genera un lazo de confianza.

(RIDMX): ¿En tema de seguridad: el gobierno está implementando algunas medidas para combatir dicho delito en los **NNA**? ¿Cuáles son estas?

(GNP): Hay una iniciativa por parte de la **RENAPO** para enrolar a los niños, de hecho se han realizado esfuerzos en las escuelas, obviamente se tenía que pedir el permiso al padre o tutor, hubo quienes accedieron y otros no, ese esfuerzo culminó con la fabricación de tres millones de Cédulas de Identidad, mismas que posteriormente se mandaron a destruir. El problema que veo en nuestro país es que se crea algo, una acción, se lleva a cabo pero nunca se usa, no se implementa y luego se tira. Y es una fortuna mandar a hacer tres millones de tarjetas de identidad, que además son muy costosas por los esquemas de seguridad que debe llevar una credencial.

Hasta donde sé no hay nada más que esfuerzos, igualmente por parte de **RENAPO**, en donde se pretende conectar todos los registros civiles y a partir de ahí se realice una enorme base para crear una identidad. Ahora bien, lo que me preocuparía como ciudadano, es el tema de la privacidad, la mía y sobre todo la de mis hijos. Porque siempre habrá quien quiera manipular de mala manera tu información. Nuestra labor como sociedad será la de buscar la manera de blindar estos esquemas y así protegernos.

(RIDMX): La sociedad mexicana, en específico los padres de familia ¿están conscientes de la problemática que surge en temas de seguridad y robo de identidad con los **NNA**?

(GNP): **No, definitivamente no creo que haya consciencia.** Es muy sonada la cuestión de "si antes jugabas en la calle o no", una actividad que hoy en día ya no se da, no existe. Creo que más bien ahora hay "miedo" o "pánico" acerca del tema de robo de menores. En este escenario veo a las personas más "espantadas", por llamarlo de alguna manera, y cada vez hay más miedo en la población. Pero en cuanto a **Robo de Identidad** aún no se aterrizan las implicaciones que puedan generar dicho delito y me atrevo a decir que no está ni estudiado, ni concientizado y es una cuestión en la que deberíamos analizar más a fondo las implicaciones que pudiera llegar a generar.

Hay un caso de una persona que trabajaba en una inmobiliaria, en la venta de casas, un día fue a mostrar una y desapareció, poco tiempo después la encontraron sin vida. La situación tan peligrosa que se está viviendo en el país, entonces deberíamos no sólo enfocarnos en los **NNA** que obviamente son importantes pero el riesgo va mucho más allá. Al hablar de este ejemplo en específico, las inmobiliarias deberían tener doble responsabilidad en el tema de identidad: uno para la prevención de lavado de dinero, que incluso hay leyes que lo regulan, y otra de proteger a sus empleados, autenticando a sus posibles compradores, porque literalmente los "avientan" con "quién sabe quién". Estos actos se podrían evitar, lamentablemente no es así, ya sea por la negligencia de las instituciones, en este caso de las inmobiliarias, o porque no quieren o porque no saben, y es que la negligencia se puede confundir fácilmente con ignorancia. Otro ejemplo son las líneas de prepago, no podemos saber cuántas líneas están registradas a nuestro nombre, si sólo existe la que utilizamos nosotros o hay otras diez dentro de los reclusorios. El tema de los **NNA** es muy importante, desde el punto de vista preventivo, pero con quien ya tenemos problemas conocidos, a los que ya se les roba la identidad, es los mayores de 18 años.

(RIDMX): ¿Existen soluciones digitales o análogas para prevenir el **Robo de Identidad**? Si las hay, **¿cuáles son?** y si no existen, **¿sabe si se está desarrollando alguna?**

(GNP): Tecnológicamente hay varias, me enfocaré desde el punto de vista biométrico, la biometría tiende a cambiar en el ser humano. Obviamente los niños son los que más cambios tienen, en un pequeño periodo de tiempo de los 0 a los 18 años tienes una sucesión de eventos y cambios de muchos tipos. Biométricamente dejas de ser "tu" cada año y cuando eres bebé prácticamente casi cada mes, porque cambian las facciones, los dedos, la voz. Conforme se van acercando a la mayoría de edad van reduciendo los cambios y se podría usar la tecnología biométrica para identificar a una persona de una manera más certera. Hay tecnologías que te pueden garantizar que, aproximadamente después de los 8 o 10 años, se puede generar una identidad, sin duda es importante esta creación de una Identidad Digital en los niños pero para ello primero se deberá generar la del padre porque a final de cuentas tienes que ligar la identidad con el tutor (tema legal), y para ello primero se debería generar la base de identidad de la persona responsable.

Ahora bien, la biometría más certera es el **ADN**, pero eso no significa que a cada niño que nace se le pida una muestra de sangre y la metas en un banco de **ADN** porque no puedo imaginar la serie de problemas que tendría la institución a cargo de ello, en el tema de privacidad, ya que tendría la base de datos de todo el país, si ocurriera algún problema sería muy grave porque una vez que te roban la identidad, ese dato que te robaron, lo robaron para siempre.

(RIDMX): ¿Deberían existir algún programa social para prevenir y combatir el **Robo de IDentidad** en los **NNA**?

(GNP): Más allá de ser obligación de las empresas creo que nosotros como ciudadanos deberíamos empezar a exigir que la **Identidad Digital** de cualquier servicio sea tomada con responsabilidad por parte de las empresas. Desafortunadamente cuando hablas de **Robo de IDentidad** creas consciencia a través del caos. Hay dos formas de vender "algo", "lo que sea", en este mundo: a través de la felicidad y a través del miedo. Nosotros nos enfocamos en un escenario tan malo que dices: "no importa cuánto hay que pagar por mi seguridad". Por ello debemos concientizar a las personas, para entender por qué los datos de identidad son importantes para cada uno de nosotros, como debemos cuidar nuestra identidad y exigir a las empresas que cuiden nuestros datos

(RIDMX): ¿Cuáles son los esfuerzos por prevenir el **Robo de IDentidad**, por parte de las empresas?

(GNP): El problema es que para poder acceder a ciertas cosas debemos seguir las normas y lineamientos establecidos, por ejemplo: si yo no accedo a dar mis datos al buró de crédito, no me van a dar un crédito, lo que me autorizarían sería un monto mínimo. Todo se vuelve un condicionante para acceder a nuestros datos.

El **aviso de privacidad** que se utiliza ya en la mayoría de las empresas en donde dejas datos, está bien porque se cumple con un marco legal, oficial; se supone que dichas empresas están certificadas en cómo deben de tratar nuestro datos, pero realmente nada nos lo garantiza. Por ejemplo: los Call Center, que llaman muchas veces al día y saben todos nuestros datos: nombre, dirección, hasta en que banco tenemos cuenta. ¿Cómo accedieron a dichos datos? no es un tema de la banca, es un tema de los Call Center que no sabemos de dónde tomaron nuestros datos.

Y es que no tenemos la cultura de cuidar nuestra privacidad, como en las Redes Sociales, le terminamos dando que "si" a todo con tal de estar dentro y no nos fijamos realmente en la cantidad de datos que damos a los demás, fotografías, ubicaciones, etc. Como usuario, no nos detenemos a leer nada, si realmente leyéramos las políticas de privacidad e hiciéramos consciencia, seguramente no las usaríamos. Las redes saben dónde estás en este momento, las compañías de telecomunicación también saben dónde estás.

Las redes sociales trabajan así: te ponen una zanahoria, esa zanahoria que todo el mundo quiere y entonces te obligan a que tu des toda la información con tal de poder recibir esa zanahoria.

Es muy grave todo lo que se puede saber a través de la tecnología, que fue creada para hacer el bien y facilitar la vida al ser humano, aunque también puede ser llevada por el contrario y hacer el mal. Desde el punto de vista preventivo la tecnología se podría emplear para identificar delincuentes y a todos los que estén vinculados pero entra la disyuntiva ¿qué hacer? No se puede encerrar a todo aquel que este en contacto con dicha persona, se vuelve un tema de seguridad nacional, de privacidad.

El reto que tiene todas las instituciones es el de garantizar y generar la identidad de sus usuarios, lo cual no siempre es posible, porque existe el tema del "hasta dónde": ¿hasta dónde quieres llegar como institución?, ¿hasta dónde quiere llegar el gobierno en tema de normatividad? ¿hasta dónde quiere llegar el usuario, en el tema de aceptación? Y sobre todo, ¿qué datos te voy a dar y cómo lo vas a cuidar?

(RIDMX): ¿Cómo está trabajando el **FIMPE** en 2019 para mejorar la situación?

(GNP): En el **FIMPE** hay total transparencia porque los participantes son instituciones financieras. Es un fideicomiso creado sin fines de lucro que genera soluciones, establece términos de competencia económica y sobre todo lo que hacemos e impulsamos, son soluciones verdaderas. Entendemos que en todos los sectores hay muchas competencias, que hay muchos participantes en cada uno de ellos pero en donde no vemos que hay una igualdad es en el tema base, en la relación que existe en todas las instituciones para hacer que todos los participantes colaboren. La **FIMPE** es un motor, es una institución que promueve mucho el tema de la interoperabilidad y la colaboración sin importar el sector y el tamaño de la empresa. Pues no hay un sector que este libre del tema de **Robo de IDentidad**.

(RIDMX): ¿Qué retos y mejoras encontraremos en este año?

(GNP): Se debe crear conciencia tanto en las instituciones como en los usuarios, que el usuario exija a las instituciones tener métodos de autenticación lo más certeros posible. Desde el punto de vista legal: revisar hasta dónde puedes llegar sin entrar en temas de privacidad, derechos humanos, etc.

El **Robo de IDentidad** existe en todos los sectores, la diferencia es que antes era más difícil, como ahora todo es digital es mucho más sencillo hacerte pasar por alguien que no eres. Cuando nosotros realizamos una operación, no sabemos si del otro lado las empresas son reales, pero no sólo es problema del usuario hacia las instituciones también es al contrario y la única manera de romper con este círculo es generando Identidades Digitales y empezar a utilizarlas. **El reto de este siglo es el tema de la privacidad, porque la tecnología ya existe, el tema es ¿cómo la aseguramos?**

RESEÑA:
LANZAMIENTO DE ROBO DE IDENTIDAD MX

El pasado miércoles 10 de abril de 2019 se presentó, en la Torre Latino Reforma, la **Revista Digital Robo de Identidad MX**.

Se trató de un evento que contó con la presencia de diferentes expositores, expertos en el tema, que nos brindaron conferencias, cursos y talleres. Entre las ponencias se encontró la de **Mario Di Costazo**, Ex Presidente de la CONDUSEF, **Gueorgui Nikolov**, Director General del FIMPE, **Carlos Provencio**, Delegado de la AMFE, **Adrián Cervantes**, Experto en Tecnologías Biométricas, **Elsa Ayala**, Consultora Independiente, **Luis Lemus** y **Mauricio Sánchez**, Socio y Abogado respectivamente de la firma Calderón & de la Sierra e **Iván Rodríguez**, Director General de Medici y también de esta nueva revista.

Robo de IDentidad MX es un proyecto que nace por la necesidad de informar a empresas y a la población en general, acerca de este mal del que todos podemos ser víctimas con el fin de informar y ayudar a protegernos de dicho delito.

¿CÓMO CUIDAR LA IDENTIDAD DE LOS NIÑOS?

¿SABÍAS QUE TODOS PODEMOS SER VÍCTIMAS DEL ROBO DE IDENTIDAD? PROTEJAMOS A NUESTROS NIÑOS.

En ocasiones escuchamos que a alguien le clonaron la tarjeta, le hicieron cargos que no reconoce como el de un crédito automotriz para un auto de lujo, una hipoteca que no es suya o que está relacionado con un delito grave, sin embargo, no pensamos en el daño que dicho suceso les está ocasionando, que cambia por completo su entorno y modo de vida. Esto mismo puede sucederle a tus hijos o los hijos de alguien más, ya que, debido la digitalización del mundo, los niños son más vulnerables a sufrir un robo de identidad y esto les afectará sus vidas de una forma inimaginable.

El **Robo de Identidad** se identifica como la utilización de datos personales que constituyen la cédula de otra persona como: nombre, teléfono, domicilio, fotografías, huellas dactilares, números de licencia y seguridad social, números de tarjeta de crédito y cuentas bancarias, nombres de usuario y contraseñas.

MÉXICO ocupa el octavo lugar, a nivel mundial, en cuanto al delito de **Robo de Identidad**:

67% **por pérdida de documentos**

63% **por robo de cartera**

53% **por información tomada de una tarjeta bancaria**

Dicho delito se usa para la obtención de una línea de crédito, contrato de línea de teléfono, realizar compras en línea y en algunos casos para el cobro de seguros de vida y pensiones.

En la actualidad nuestros datos personales están mucho más a la mano de personas que pueden hacer mal uso de ellos, sin embargo, hay medidas que los bancos, el gobierno, las redes sociales, etc. implementan y mejoran día con día, pero,

¿QUÉ HAY DE NUESTROS NIÑOS?

La *Ley General de los Derechos de Niñas, Niños y Adolescentes* en su **capítulo tercero, artículo 19, sección IV**, habla acerca del cuidado de la identidad de los niños como ciudadanos de nuestro país:

> *"Preservar su identidad, incluidos el nombre, la nacionalidad y su pertenencia cultural, así como sus relaciones familiares. Las autoridades federales, de las entidades federativas, municipales y de las demarcaciones territoriales del Distrito Federal, en el ámbito de sus respectivas competencias, deberán colaborar en la búsqueda, localización y obtención de la información necesaria para acreditar o restablecer la identidad de niñas, niños y adolescentes"*

Una investigación realizada por **Javelin Strategy & Research** muestra que durante 2018 **más de un millón de niños fueron víctimas de robo de identidad** y de ellos, dos terceras partes tenían de 0 a 7 años de edad. Estas cifras son alarmantes porque además de vivir en un mundo de constantes cambios y peligros, ahora también se le suma el estar expuestos a ser víctimas de robo de identidad. Y aún más alarmante es que seis de cada diez de estas víctimas conocen al responsable.

Por otro lado, el no tener una identificación oficial o cuenta de banco, los hace ser blanco fácil y estar completamente expuestos a esta nueva manera de extorsión. La facilidad que proporciona el no tener una "Identidad" ante el estado, da al defraudador la posibilidad de crear una nueva línea de crédito, crear un perfil en redes sociales falso, abrir una cuenta de correo electrónico y, en resumen, hacer uso de dicha identidad para cualquier cosa que le apetezca.

El banco mundial estima que más de **1,1 billones de personas en todo el mundo no cuentan con una forma oficial de identificación** y de todas ellas la mitad viven en:

Bangladesh **China** **India** **Indonesia** **Nigeria** **Pakistán** **México**

Esta falta de prueba de identidad genera a su vez **exclusión política, social y económica**.

En México, al menos, **no eres nadie hasta que cumples la mayoría de edad** ,creando un blanco fácil para cometer el delito de suplantar la identidad de alguien.

Es por ello que la *Ley General de los Derechos de Niñas, Niños y Adolescentes*, de la cual hablamos antes, consta de un apartado completo donde se habla de la protección de datos personales en los menores:

ARTÍCULO 76

"Niñas, niños y adolescentes tienen derecho a la intimidad personal y familiar, y a la protección de sus datos personales. Niñas, niños y adolescentes no podrán ser objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia; tampoco de divulgaciones o difusiones ilícitas de información o datos personales, incluyendo aquélla que tenga carácter informativo a la opinión pública o de noticia que permita identificarlos y que atenten contra su honra, imagen o reputación.

Quienes ejerzan la patria potestad, tutela o guarda y custodia, deberán orientar, supervisar y, en su caso, restringir, las conductas y hábitos de niñas, niños y adolescentes, siempre que atiendan al interés superior de la niñez."

¿CÓMO SABER SI MI HIJO ES VÍCTIMA DEL ROBO DE IDENTIDAD?

Es importante saber y tener en cuenta las medidas que se deben de llevar a cabo para saber si nuestros pequeños están siendo víctimas de este delito. La mejor manera es:

Investigar si existen archivos de crédito a nombre de los pequeños.

Verificar que no se encuentre en Buró de Crédito.

Googlear su nombre por lo menos una vez cada seis meses.

Guardar en un lugar seguro los registros impresos y electrónicos que contengan información personal de su hijo.

Romper todos los documentos que contengan información de su hijo antes de tirarlos a la basura.

Es importante platicar con nuestros hijos acerca de los riesgos que se corren, de cómo proteger su información, enseñarles a utilizar el Internet de manera segura y a saber detectar posibles fraudes y estafas. De igual forma el estar al tanto de cuál es la información personal que almacenamos de ellos en nuestros dispositivos electrónicos y lo que compartimos con personas ajenas.

Una de las más grandes soluciones siempre será la comunicación con nuestros hijos para que las estadísticas, que son muy alarmantes, no crezcan en el rubro de robo de identidad infantil. Crear conciencia y que surja esta "educación" sobre la importancia de proteger la identidad en niños, niñas y adolescentes, con ello lograr la prevención y con el tiempo mitigar dicho delito para que no cambie la vida de aquellos a quien tanto amamos.

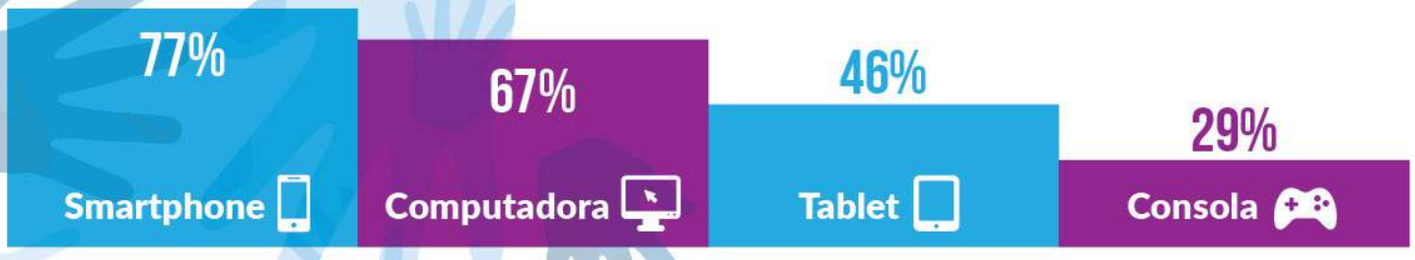
Si se llegase a encontrar bajo alguno de los supuestos de fraude, es importante que cuanto antes se ponga en contacto con algunas de las entidades que les puedan proporcionar la debida orientación y ayuda: **CONDUSEF, PROFECO y la Policía Federal**.

Fuentes:
- Comisión Nacional para la Protección y Defensa de Usuarios de Servicios Financieros (CONDUSEF).
- Fondo de las Naciones Unidas para la Infancia (UNICEF).
- Federal Trade Commission (FTC).
- National Broadcasting Company (NBC).

INFOGRAFÍA: LOS NIÑOS Y LA SEGURIDAD EN INTERNET

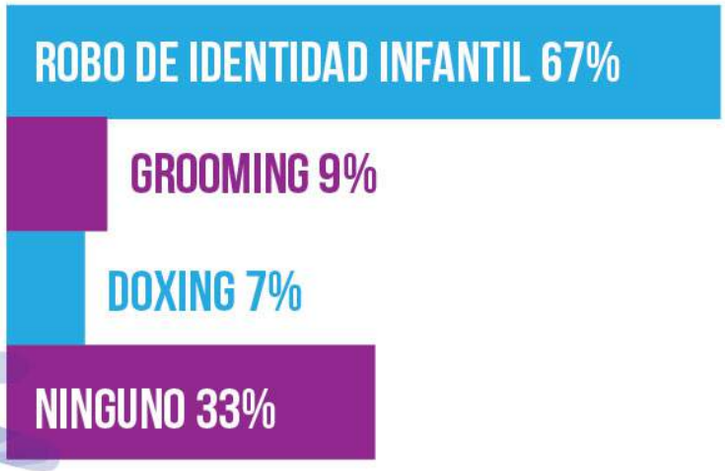
La siguiente encuesta se llevó a cabo en el sitio web de **Robo de IDentidad MX**.

¿Con cuántos dispositivos **interactúan tus hijos**?



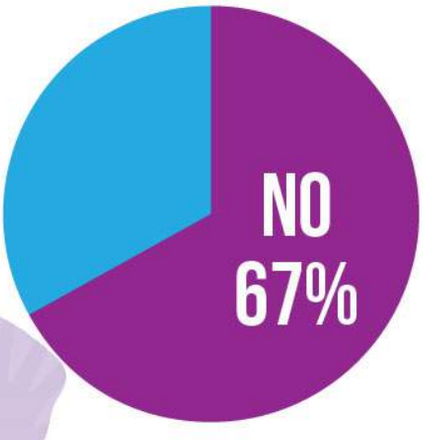
¿Manejas **control parental** en los dispositivos que utilizan tus hijos?

¿Has escuchado los siguientes **términos**?



Tu hijo cuenta con:

¿Tú **le ayudaste** a tu hijo a crear sus **redes sociales**?



¿Sabes **qué hacer** si te **roban la identidad**?

Agradecemos a todas las familias que nos ayudaron participando en esta encuesta.

EL ROBO DE IDENTIDAD es una AMENAZA que se vuelve MÁS GRANDE día con día

Para combatirla, presentamos:

PIMA

Plataforma de Identidad Multibiométrica A.C.

Con base en la experiencia de las empresas que componen **PIMA**, hemos diseñado una plataforma que permitirá conectar con más de 100 elementos de verificación de una sola identidad de forma simple y segura.

La plataforma combina tecnología de **última generación en identidad digital, biometría e inteligencia artificial**, apegado a estándares de la industria, los que aplican por parte de la **CNBV** y otras instituciones públicas que verifican identidades biométricas o documentales.

Garantizamos mitigar fraudes con **retornos de inversión a corto plazo** por disminución de costos y por incremento de utilidad. Le permitirá verificar la identidad de su cliente con otras instituciones pertenecientes a la **AMFE**, identidades biométricas de bancos, 95% de los correos electrónicos a nivel mundial y a más de 250 millones de identidad digitales.

PIMA ha creado flujos específicos que permiten validar la identidad de sus prospectos o clientes de una forma amable, segura y permite acelerar la **transformación digital** de los negocios.

PIMA potencializa las campañas de marketing digital haciendo el proceso de ventas más rápidos. Protege la reputación de su financiera, previniendo fraudes por robo de identidad y permitirá ofrecer mayores beneficios para los clientes que cuenten con una identidad verificada por el ecosistema.

Nuestra plataforma permite **acelerar tu transformación digital**, **prevenir fraudes** y **cumplir con tus regulaciones** por medio de su **ecosistema en servicios de identidad**.

Validación de identidad y biometría

Obtén y valida la **identidad biométrica de tus clientes** y genera una **base de datos segura**.

IDentidades Digitales

Verifica y conecta con las **IDentidades Digitales** creadas por el **ecosistema PIMA**, el cual esta compuesto por mas de 40 entidades financieras, 2.5 millones de identidades digitales, 95% de los correos electrónicos globales.

Conexión con Bases de Datos de Gobierno

Verifica la identidad **conectando** con servicios y bases de datos del gobierno.

Cumplimiento Regultatorio

Da cumplimiento a regulaciones **CUB, PLD, CNBV, FINTECH, SOFOM, CONSAR**.

Firma Electrónica

Firma digitalmente tus contratos y solicitudes haciendo legalmente admisibles los documentos por medio de la **NOM151**.

Contratos Digitales

Elimina el papel y **realiza contrataciones desde cualquier dispositivo** de forma electrónica, genera formularios y verifica identidad para **vender más**.

PIMA

Plataforma de Identidad Multibiométrica A.C.

(55) 9191-6788

(55) 5434-4438

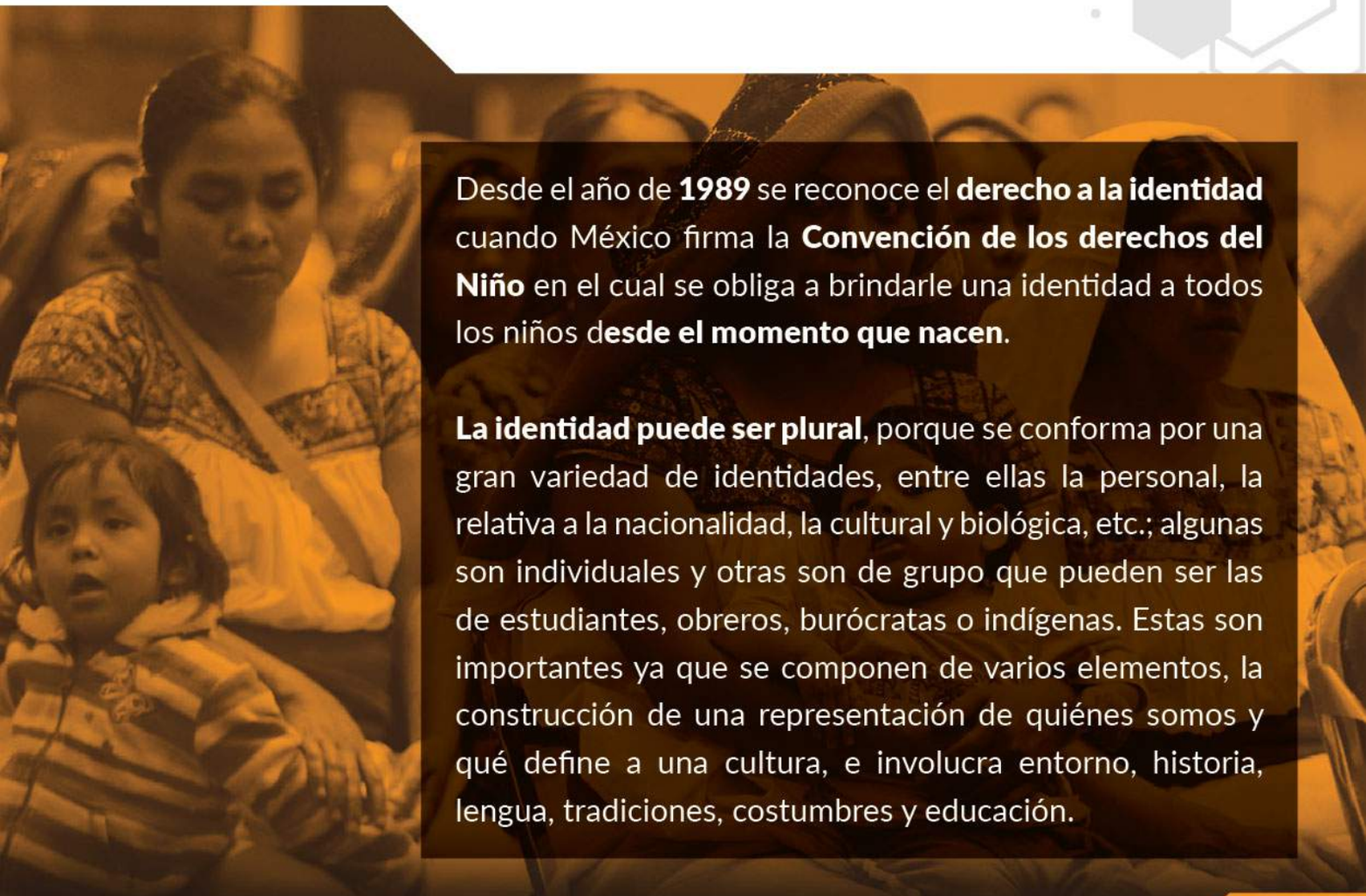
ventas@robodeidentidad.mx

LA IDENTIDAD Y LOS PUEBLOS INDÍGENAS

Por: Vanessa Martínez Mandujano

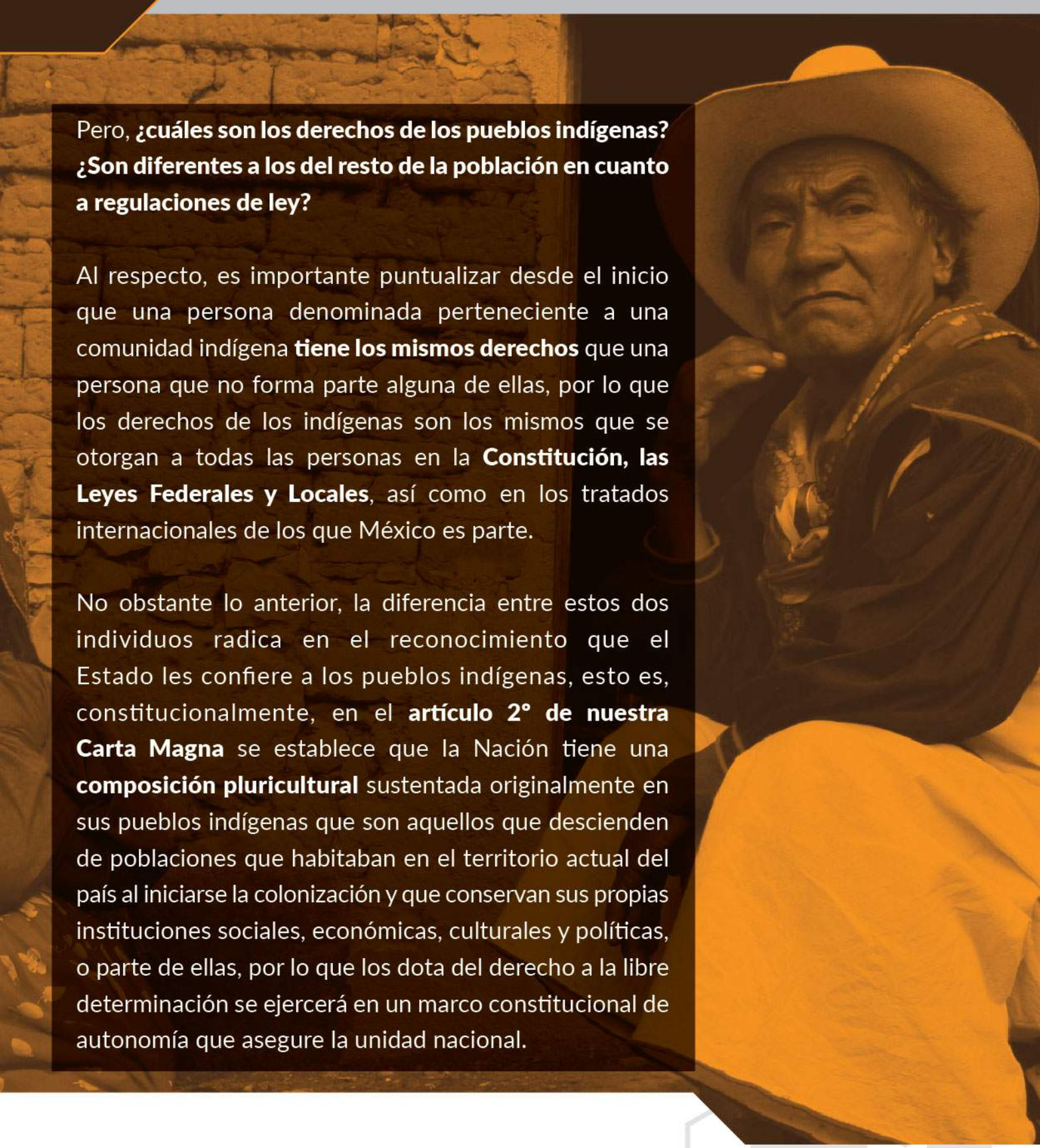
Según la RAE, **la Identidad** se define como "el conjunto de rasgos que caracteriza a un individuo o a una colectividad frente a los demás. En el primer caso, el individual, resalta el hecho de que cada individuo es único y diferente debido a las particularidades comunes que distinguen a los seres humanos del resto del reino animal. En el segundo caso, el colectivo, una persona se representa como tal cuando se reconoce a sí misma y a otras personas como miembros de una comunidad. Esta última, a su vez, aunque comparte similitudes con otras comunidades tiene rasgos que la diferencian."

Tiene que ver con sus antecedentes familiares, lo que implica tener un **nombre, apellido y nacionalidad**. Desde que nacemos tenemos **el derecho a tener una identidad**, el cuál junto con la protección del individuo es el eje sobre el cual giran los otros derechos que definen a una persona humana y están ínfimamente relacionados con el derecho a la salud, a la intimidad, a una vida digna, a la libertad de creencias religiosas, libertad de pensamiento, libertad de opinión y a no ser discriminados.



Desde el año de **1989** se reconoce el **derecho a la identidad** cuando México firma la **Convención de los derechos del Niño** en el cual se obliga a brindarle una identidad a todos los niños d**esde el momento que nacen**.

La identidad puede ser plural, porque se conforma por una gran variedad de identidades, entre ellas la personal, la relativa a la nacionalidad, la cultural y biológica, etc.; algunas son individuales y otras son de grupo que pueden ser las de estudiantes, obreros, burócratas o indígenas. Estas son importantes ya que se componen de varios elementos, la construcción de una representación de quiénes somos y qué define a una cultura, e involucra entorno, historia, lengua, tradiciones, costumbres y educación.



Pero, **¿cuáles son los derechos de los pueblos indígenas? ¿Son diferentes a los del resto de la población en cuanto a regulaciones de ley?**

Al respecto, es importante puntualizar desde el inicio que una persona denominada perteneciente a una comunidad indígena **tiene los mismos derechos** que una persona que no forma parte alguna de ellas, por lo que los derechos de los indígenas son los mismos que se otorgan a todas las personas en la **Constitución, las Leyes Federales y Locales**, así como en los tratados internacionales de los que México es parte.

No obstante lo anterior, la diferencia entre estos dos individuos radica en el reconocimiento que el Estado les confiere a los pueblos indígenas, esto es, constitucionalmente, en el **artículo 2° de nuestra Carta Magna** se establece que la Nación tiene una **composición pluricultural** sustentada originalmente en sus pueblos indígenas que son aquellos que descienden de poblaciones que habitaban en el territorio actual del país al iniciarse la colonización y que conservan sus propias instituciones sociales, económicas, culturales y políticas, o parte de ellas, por lo que los dota del derecho a la libre determinación se ejercerá en un marco constitucional de autonomía que asegure la unidad nacional.

LOS PUEBLOS INDÍGENAS Y SUS DISTINCIONES

Por definición **la Constitución** establece que son "comunidades integrantes de un pueblo indígena", **aquellas que formen una unidad social, económica y cultural**, asentadas en un territorio y que reconocen autoridades propias de acuerdo con sus usos y costumbres. Para entender más ampliamente esta definición existen diferentes criterios para considerar o determinar quiénes son actualmente personas indígenas.

Básicamente son **tres elementos** los que, dependiendo de las consideraciones de cada Institución, se establecen como **definitorios**:

Al respecto el **Instituto Nacional de Estadística y Geografía (INEGI)**, define la condición de habla indígena como la **"Distinción de la población de 3 y más años de edad según declare hablar o no alguna lengua indígena"**, aunque este criterio tiene una falla pues excluye a las personas de tradiciones indígenas cuya lengua se ha perdido a través de las generaciones.

Se refiere a reconocerse como tal, esto es, **el autorreconocimiento como persona indígena** con base en su propia **cultura, tradiciones e historia**.

En este punto la **Comisión Nacional para el Desarrollo de los Pueblos Indígenas (CDI)**, considera que siendo el hogar la institución principal de socialización, transmisión cultural y conformación de la identidad considera población indígena a todas las personas que lo conforman cuando uno de sus integrantes **se haya declarado ser hablante de lengua indígena**, por lo que, si bien se considera como criterio principal el lenguaje, **tiene la posibilidad de integrar a quienes no la manejan**.

EL ROBO DE IDENTIDAD EN LOS PUEBLOS INDÍGENAS.

La ONU declaró este 2019 como el **año internacional de las lenguas indígenas**. En la República Mexicana, **25 millones de personas que se reconocen como indígenas**; sin embargo, en temas de robo de identidad **no existe ninguna ley específicamente creada para atender a dichas comunidades**, es decir, el marco normativo existente para identificar, evitar y erradicar el robo de identidad es el mismo que para cualquier ciudadano o persona que se encuentre en territorio nacional. Por otro lado, tampoco existe un sitio web específicamente creado para atender este tema, pero si existen el sitio oficial del **Instituto Nacional de los Pueblos Indígenas y de la Comisión Nacional para el Desarrollo de los Pueblos Indígenas**, mediante los cuales se pueden realizar quejas y denuncias por parte de las personas pertenecientes a los pueblos indígenas respecto a su identidad, por lo que, si bien no se protege el robo de identidad como comúnmente lo conceptualizamos, el Estado al intentar proteger y salvaguardar la identidad de los pueblos indígenas, puede de manera indirecta (no creado medios o procesos específicos) y extensiva atender este tema.

Finalmente, como **opinión personal**, es imperante entender que la condición especial que guardan los pueblos y comunidades indígenas es respecto a sus usos y costumbres, **a fin de preservar la herencia cultural e histórica del país**, por lo que legalmente no debe existir distinción al proteger la identidad de un individuo. Es decir, no deben existir leyes o normas especiales para proteger este atributo de la persona, pero si deberían crearse los mecanismos idóneos para equilibrar y hacer efectiva la igualdad de condiciones entre personas consideradas indígenas y el demás grueso de la población.

Vanessa Martínez Mandujano es abogada de la **Escuela Libre de Derecho** quien realizó una extensa investigación parte de su tesis de titulación llamada **"Ineficacia de los organismos especializados para la protección de los derechos humanos de las comunidades indígenas"**.

Fuente:
- Comisión Nacional de los Derechos Humanos (CNDH).
- Instituto Nacional de Lenguas Indígenas (INALI).

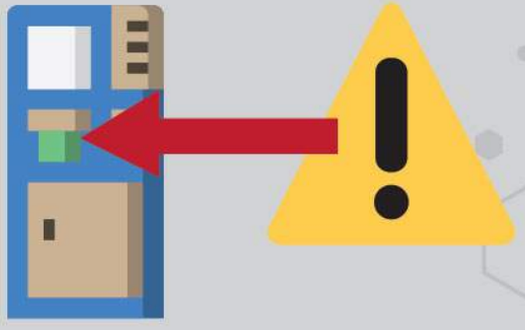
PRO TIPS: ¿CÓMO PROTEGER TU ID ENTIDAD?

6 TIPS FÁCILES DE SEGUIR

1

Evita proporcionar **información personal o financiera** por teléfono.

2



Al acudir al **cajero automático** revisa que no cuente con **dispositivos extraños**.

3

Al pagar con tarjeta **no la pierdas de vista**, solicita que **te lleven la terminal** al lugar donde estés.

4

Revisa constantemente tus **estados de cuenta** para que verifiques que los cargos **correspondan a los que hayas realizado**.

5

Protege tus contraseñas, no las escribas en tu celular o en algún lugar visible para otras personas.

6

Haz caso omiso de mensajes en los que te comuniquen que has ganado un premio o te hacen una oferta especial.

ACCOUNT TAKEOVER: QUÉ ES Y CÓMO PREVENIRLO

Por: José Caldera

INTRODUCCIÓN

El robo de cuentas **(Account Takeover – ATO por sus siglas en inglés)** sucede cuando un criminal toma control de la cuenta de un usuario legítimo, usualmente de manera temporal, para realizar actividades ilegales o como paso intermedio para ocultar su identidad real.

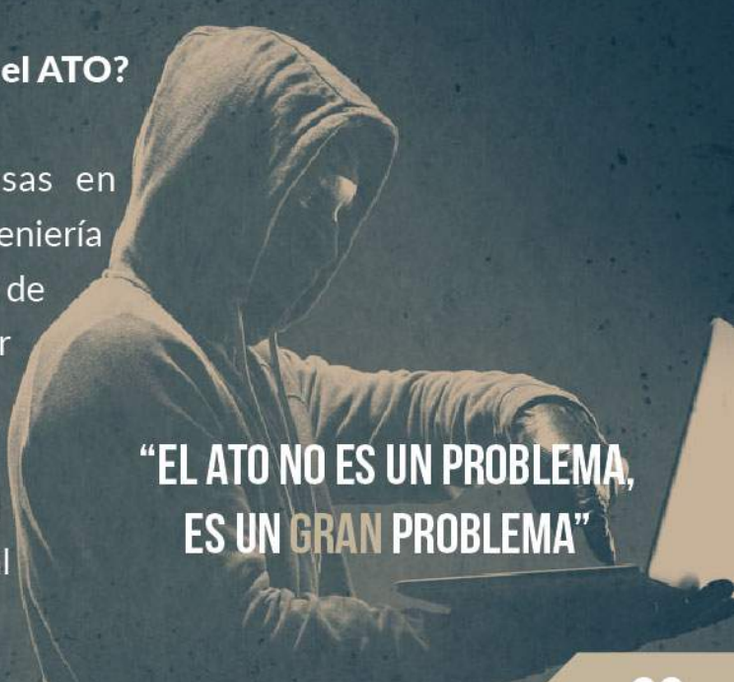
"El costo del **ATO** se triplicó durante el 2017, llegando a un estimado de $5.1 Billones en los Estados Unidos". En el reporte del grupo Aite, *"Machine Learning: Fraud Is Now A Competitive Issue"*, **casi todas las instituciones financieras entrevistadas incluyeron robo de cuentas como uno de sus primeros problemas**.

El **ATO** no es tan complicado de detectar y prevenir. Hay muchas formas y técnicas disponibles que son fáciles de implementar. La pregunta que los grupos de riesgo, fraude y cumplimiento deben hacerse es cuánto deben gastar en prevenirla, y qué tan importante es para su organización. La respuesta, naturalmente, depende del análisis de riesgo. Por ejemplo, un sitio de comercio electrónico lidiando con una posibilidad de fraude de $100 es muy diferente al riesgo de un criminal que en segundos puede transferir miles de dólares de una cuenta bancaria.

BACKGROUND

Empecemos desde el principio: **¿Cómo sucede el ATO?**

La forma más común, como todas las cosas en ciberseguridad, emplea alguna forma de ingeniería social. Ingeniería Social se define como: "El uso de decepción para manipular individuos en divulgar información personal y confidencial que puede ser utilizado para cometer fraude." En términos prácticos, las dos formas más comunes son el "*phishing*" e interacciones falsas con ayuda al cliente.



El nivel y los esquemas de decepción pueden ser muy sofisticados, pero fundamentalmente se resumen en: lograr que la víctima dé la información necesaria para que un criminal pueda autenticarse (robarse la contraseña) o dar la información para que el criminal pueda cambiar los procesos de autenticación disponibles en la aplicación (cambiar la contraseña de la cuenta), y así poder tomar control de la cuenta.

Adicionalmente, la cantidad de robo de data a gran escala ha facilitado un canal adicional para el robo de credenciales: "*The Dark Web*". Obtener credenciales en el "*dark web*" es fácil y barato. Estas credenciales se utilizan para cometer un tipo de ataque conocido como "*Credential Stuffing*". En muchos casos los datos personales de individuos vienen con contraseñas en texto simple, e independientemente de dónde vengan los datos, usuarios comúnmente utilizan las mismas contraseñas para autenticarse en diversas aplicaciones. Entonces las oportunidades de que las mismas contraseñas sean válidas son muy altas. Los criminales utilizan estas combinaciones de cuentas y contraseñas para automatizar sus ataques a gran escala (*credential stuffing*) y lograr acceso a las cuentas de las víctimas.

Hay muchas técnicas para prevenir el **ATO**, pero la más común y más utilizada se centra en los métodos de autenticación, ya sea multifactor **(MFA)**, contraseñas de uso único, bloqueo de cuentas ante múltiples pruebas fallidas, mecanismos de cambio y recuperación de contraseñas basados en conocimiento previo. Bloquear una cuenta en condiciones de fallas múltiples es efectivo, pero también problemático para los usuarios, ya que no les gusta tener que cambiar la contraseña cuando se les olvida. Preguntas basadas en conocimiento previo es una técnica muy utilizada, pero con el tiempo ha probado no ser efectiva. Más aún con la proliferación de robo de datos de identidad.

Hay técnicas más sofisticadas para prevenir el **ATO** que incluyen el monitoreo activo de cuentas de usuarios y más específicamente en alertar cuando hay cambios en las cuentas. Por ejemplo, cuando un usuario añade un nuevo destino para transferencia electrónica de dinero, o cuando se cambia las dirección de domicilio, etc. Muchas entidades financieras y sitios de comercio electrónico alertan a los usuarios a través de mensajes de texto o por correo electrónico cuando estos cambios suceden. Sin embargo, estas configuraciones de las cuentas no son obvias para los usuarios y muchas veces no son correctamente configuradas. El resultado, es que dichas alertas son sólo efectivas al nivel en que los usuarios las entiendan y activen. Adicionalmente, mientras más transacciones ejecute el consumidor, deberá ser mayor la cantidad de alertas. Manejar estas configuraciones a través de todas las cuentas es difícil e inconveniente.

Una técnica menos intrusiva es monitorear el comportamiento del usuario en la aplicación. Ritmos de escritura, navegación en los sitios en línea e interacciones con las aplicaciones que pueden ser monitoreadas para establecer patrones de uso y luego comparar contra esos patrones. Sin embargo, estas técnicas pueden ser costosas de implementar y mantener, dado que tendrán que ajustarse cada vez que haya cambios en las experiencias de usuarios en las aplicaciones, lo cual implica revisión de los patrones. La **Biometría de Comportamiento** ha evolucionado mucho en los últimos años, se ha vuelto un poco más efectiva, y fácil de implementar. Vale la pena considerar esta técnica sólo por el valor "*out-of-the-box*" de detectar ataques automatizados.

Finalmente, también está el monitoreo de transacciones en tiempo real. Datos de la transacción pueden ser utilizados para crear patrones como cambios en acceso geográfico, dispositivos, direcciones de envío, tipo de productos, nivel de gasto y hábitos de consumo. Estos cambios pueden indicar actividad sospechosa, que puede a su vez detectar que los usuarios son distintos a los dueños de las cuentas.

DEFENDER Y PREVENIR EL ACCOUNT TAKEOVER CON LA PLATAFORMA DE IDENTIDADES DIGITALES DE IdentityMind

IdentityMind es pionero en el uso de identidades digitales. A través de su tecnología patentada **Electronic DNA™ (eDNA™)**. El **eDNA™** de un usuario digital es una representación que incluye:

Atributos digitales como la dirección de correo electrónico, número telefónico, dispositivos de conexión, redes sociales, ubicación geográfica basada en dirección IP.

Atributos físicos como el nombre, dirección domiciliar y de envío, documentos de identidad.

Información de pagos, es decir, tarjetas de crédito, número de cuentas bancarias, monederos electrónicos.

Data biométrica, selfies, comportamientos, huellas

Comportamientos, acceso, login, pagos.

Esta combinación de atributos y comportamientos son validados a través de heurísticas, machine learning y fuentes externas. El **eDNA™** es la base para aplicar todas las técnicas descritas previamente para detectar y prevenir el robo de cuentas.

La eficacia de la plataforma de **IdentityMind** es el **eDNA™** que se crea para todos los usuarios. El **eDNA™** es un activo digital que persiste y se ajusta automáticamente a través de las transacciones del usuario. Cuando se complementa esto con el monitoreo en tiempo real de transacciones y la comprobación de identidades, se logra extender el valor del proceso de enrolamiento en el tiempo del usuario, y por ende la efectividad en la detección y prevención de robo de cuentas.

Los analistas que combaten riesgo y fraude pueden estar preocupados con el costo potencial y la posibilidad de fricción en la experiencia de usuario cuando se implementan técnicas de validación de identidad en el monitoreo de transacciones. Este es otro de los beneficios de la plataforma de **IdentityMind**. El **eDNA™** siempre se construye, y muchas técnicas de corroboración internas no necesitan los costos adicionales de las fuentes externas. Estos procesos internos también modelan condiciones de riesgo que pueden ser conectados con actividades de autenticación para comprobar la identidad real del usuario.

Muchas organizaciones separan el proceso de apertura de cuenta del proceso de monitoreo. Esto es ineficiente. La forma más efectiva, es cuando se integran ambos procesos de manera que uno complemente al otro.

José Caldera, con maestría en Ciencias en Redes de Información de la Universidad Carnegie Mellon, se ha dedicado a trabajar con temas de seguridad de aplicaciones y redes, también ha estado en el rubro de pagos, moneda virtual, métodos antifraude y lavado de dinero.

Desarrolló y comercializó productos para empresas como Silicon Valley, Securify, McAfee y ahora Identity Mind Global. Desde hace 20 años ha incursionado en el desarrollo y comercialización de productos y servicios para la seguridad de la información y los pagos, la mitigación de riesgos y el cumplimiento.

EL ABC DEL ANEXO 71

Por: Adrián Cervantes Jaime

28 de agosto de 2017 es una fecha que puede parecer como cualquier otra, pero se trata de la fecha en que la **Comisión Nacional Bancaria y de Valores (CNBV)** a través de la **Secretaría de Hacienda y Crédito Público (SHCP)** dio a conocer las modificaciones a diversos artículos de las Disposiciones de carácter general aplicables a las instituciones de crédito.

Esto sienta un precedente vital en la vida financiera de nuestra sociedad, ya que por medio de este instrumento el gobierno federal instrumenta las medidas para hacer frente al creciente **Robo de IDentidad en nuestro país**, definiendo los mecanismos para fortalecer la identificación de cada una de las personas que laboran en el sector financiero, así como de los usuarios de la banca.

Para lograr **este objetivo tan importante**, se plantean que instituciones de crédito **verifiquen la información** de identidad y documentación en:

Instituciones

Dependencias Gubernamentales

Entidades Gubernamentales

Por otro lado, se considera que las instituciones de crédito pueden **OMITIR** realizar las verificaciones, esto con un gran costo, que se trata de simple y sencillamente de **ASUMIR LOS COSTOS**. De igual manera es posible omitir la construcción de la base de datos biométrica, obviamente con las consecuencias que esto puede ocasionar.

Así mismo las disposiciones **consideran el uso de tecnologías de identificación** cuando se trata de operaciones sin presencia física, con esto, se abre un abanico de posibilidades en el uso de la información de datos personales que deben estar protegidos, para lo cual se establecen como mínimo el uso de estándares internacionales.

También se prevé **agilizar las transacciones** en procedimientos que ya hayan superado los procesos de identificación, es decir, aquellas transacciones en que el usuario y la institución ya tienen un mecanismo seguro donde se tiene identificado plenamente al usuario, obviando algunas validaciones, tal como sucede actualmente con el uso de tokens físicos o digitales.

El detalle de las disposiciones es muy amplio en lo correspondiente a la documentación solicitada, así como los documentos válidos para identificarse. En este sentido es importante atender minuciosamente el procedimiento, ya que se debe registrar cuando se solicita cierta información, cuando se coteja, y si se denegó algún dato.

Se establece la validación remota de la información de **RENAPO** para el caso de la **CURP**, obligando a las instituciones a llevar un control de cada una de dichas validaciones, y que deriva en la responsabilidad por la validación de la identidad de una persona.

La movilidad también se hace presente, puesto que se contempla el uso de contratación de servicios en módulos externos, mismos que deben contar con validaciones en línea. Esto amplía las posibilidades de servicios más allá de las sucursales, acercando la banca de manera segura al usuario final.

En este proceso, **la credencial para votar juega un rol importante**, pues valida la información de cada persona, así como los códigos de la propia credencial que ayudan a **verificar su autenticidad y vigencia**. En este mismo proceso se autentica la huella dactilar de la persona en vivo contra la registrada en la base de datos del **INE**.

Aunque **se requiere que la validación se realice en línea**, se prevé para casos donde no se encuentre el servicio disponible, realizar la consulta posterior, para evitar alguna posible pérdida del trámite, quedando a la espera de los resultados, lo que garantiza que **los datos estén siempre protegidos y sean utilizados para los fines específicos**.

¿Sólo el **INE** puede validar la IDentidad?

No, si alguna institución desea validar la identidad con otra entidad de gobierno, la **CNBV** revisará el procedimiento y, si es confiable, será aprobado.

¿Y el **anexo 71**?

Ya entrando en materia del **anexo 71**, se requiere de la huella dactilar, porque es un medio de identificación ampliamente probado en el que tanto legal como tecnológicamente existe el Know-How de cómo implementarlo y explotarlo.

Es claro que el procedimiento está muy detallado, porque tanto la manera de capturar, almacenar y comparar, se apoya en estándares publicados y aceptados a nivel internacional, como lo es el caso de **ISO** (*International Organization for Standardization* por sus siglas en inglés) quienes apoyados en los conocimientos de empresas dedicadas a la identificación biométrica, así como de las experiencias de instituciones y gobiernos, se han determinado protocolos para tener los mismos criterios de operación.

¿**Pixeles, profundidad, rangos dinámicos**?

Tal vez suenen muchos términos poco comunes para algunos al momento de leer las especificaciones, pero se trata de las características que las imágenes de huella deben cumplir para ser utilizadas.

Es recomendable que, al momento de la implementación de un sistema de comparación biométrica, dichas características de imágenes, flujo de información y resultados de las comparaciones, sean verificadas por un especialista. Recordemos que estamos hablando de un sistema y metodología para identificar personas y su razón de ser es realizar operaciones de manera confiable.

La metodología de operación al momento de captura es más que sólo un procedimiento. Se trata del como extraer la información más **CRÍTICA** para un sistema de comparación biométrico, ya que dependiendo de la calidad de la imagen captada será la capacidad de identificar plenamente con mejor precisión a una persona, y por ende a más huellas captadas mayor cantidad de información disponible para validar la identidad.

¿Y las **certificaciones** de los dispositivos?

Una vez que se determinó la tecnología a utilizar, es importante identificar las características que debe cumplir cada lector de huellas, por lo mismo siempre es recomendable acercarse a su proveedor de tecnología antes de realizar los procesos de adquisición y que las especificaciones sean claras.

¿Cómo sé si las imágenes **son adecuadas**?

La industria reconoce un estándar de evaluación de calidad llamado **NFIQ** (*Nist Fingerprint Image Quality* por sus siglas en inglés), este estándar cuenta con 5 valores que van desde el 1 al 5, donde el 1 es la mejor calidad en una imagen y 5 la calidad más baja.

1. Excelente
2. Buena
3. Media
4. Baja
5. Pobre

El número indica la probabilidad de que la imagen obtenga una identificación confiable. Así que es posible tener la imagen de una misma huella con distintas calidades, por lo tanto, en algunos casos podría no obtener resultados claros ni precisos.

¿Ocurre lo mismo con la **imagen facial**?

Definitivamente la imagen facial es la validación biométrica por excelencia y la que usamos de manera intuitiva los seres humanos, con ella nos reconocemos y es la que, de manera cotidiana, se revisa en credenciales, licencias, certificados de estudios, entre otros elementos que van acompañados de alguna fotografía.

Pero al momento de hablar de tecnología de identificación automática las cosas cambian un poco, ya que es necesario **realizar capturas de imágenes faciales** (fotografías) con ciertas características que involucran lo siguiente:

De igual manera como se mencionó en las huellas dactilares los protocolos están basados en estándares internacionales y en mejores prácticas de operación.

Sobre los formatos de imagen

Existen muchos formatos de imágenes digitales, pero como lo hemos visto, estos también están estandarizados y es para mantener las características de las imágenes lo más fieles a las características del rostro o es su caso a los dactilogramas, al grado de haber sido necesario la creación del formato **WSQ** que es el **Cuantificador Escalar de Ondículas** utilizado exclusivamente para el almacenamiento de imágenes de huella dactilar. Este formato fue desarrollado por el FBI para que las imágenes de huella ocuparan un espacio en memoria menor con mayor calidad.

Estándares y Terminología

La cantidad de estándares es amplia, así como los términos de uso particular, así que, si no está familiarizado con los términos y se desea adquirir equipos o soluciones biométricas, es importante acudir a un especialista pues se podrían causar confusiones al momento de la adquisición y la documentación que impactarán posteriormente en la operación.

COMUNICADO:
INCIA ACTIVIDADES LA ASOCIACIÓN DE IDENTIDAD DIGITAL MÉXICO – IDMX A.C.

"**Inicia actividades la Asociación de Identidad Digital México – IDMX AC**, creada para representar a individuos y organizaciones para difundir y fomentar las mejores prácticas en el uso de la Identidad Digital en México.

La asociación tiene como socios fundadores a **Verisec, FIMPE, ACERTA y Buró de Identidad**, quienes conforman el consejo directivo a través de sus representantes; **Carlos Flores - Presidente, Gueorgui Nikolov Popov - Vicepresidente, José Vázquez – Secretario, Pablo Vallejos – Tesorero y Emma Gaspar - Coordinadora General**.

Carlos Flores explicó que: "la asociación se crea para promover proyectos e iniciativas que involucren el uso de Identidades Digitales y ayuden a la formación de un ecosistema de Identidad Digital que beneficie a gobiernos, empresas, academia, organizaciones de la sociedad civil y al público en general".

Gueorgui Nikolov Popov puntualizó que: En México existen más de 53.4 millones de personas en estado de pobreza y los programas sociales ayudan a mitigar este problema, sin embrago, de los 6,500 programas existentes, solo uno se entregaba usando biometría, por eso, hay que trabajar en forjar una identidad digital para transparentar todos los programas de apoyo social en el país.

"La identidad digital ayuda crear una trazabilidad digital para evitar duplicidad o suplantación de identidad, además de brindar mejores servicios y atención del Estado a los ciudadanos, para tomar decisiones sobre datos reales, no estimaciones", concluyó Nikolov Popov.

José Vázquez comentó que: "Internet y las plataformas digitales son escenarios en los que interactuamos, y es fundamental contar con herramientas que permitan acreditar nuestra identidad, y entender cuándo y cómo compartir datos personales, sin que sea un riesgo a nuestra seguridad".

"Con **IDMX**, queremos poner al servicio de instituciones y ciudadanos la experiencia de expertos en temas de biometría, seguridad informática y prácticas de acreditación de identidad, para educar y fomentar la aceptación y confianza en la identidad digital", agregó Vázquez.

Pablo Vallejos dijo que: "se trabaja en construir las bases para crear un ambiente de confianza, donde se concreten estrategias que ayuden a disolver el problema de robo de identidad, y mejoren las capacidades de negociación y autenticación de ciudadanos en un futuro ".

Dando continuidad a las actividades del año pasado (www.idmx.mx), el 25 de septiembre se llevará a cabo el **Segundo Seminario de Identidad Digital en México IDMX2019**, con talleres, curso de formación de profesionales, grupos de trabajo con legisladores para desarrollar la primera legislación de Identidad Digital para México, así como impulsar iniciativas como el **programa ID4D del Banco Mundial**, y de la iniciativa **Kantara/IDpro**.

INFOGRAFÍA: ¿QUÉ ES EL DOXING? ¿CÓMO EVITARLO?

El **DOXING** es un conjunto de técnicas destinadas a **recopilar información sobre un objetivo**, ya sea una persona o una organización para después divulgarlo en internet.
Para llevarlo a cabo se recurre a **diferentes técnicas** tales como **búsquedas en bases de datos de acceso público, redes sociales y vulneración de sistemas.**

¿CÓMO EVITARLO?

Configura adecuadamente la privacidad de tus perfiles sociales

Protege tu privacidad durante las interacciones en línea. Conviértelo en una práctica habitual

Revisa siempre **si está activado tu GPS** y analiza si es necesario compartir tu ubicación en redes sociales

Mantén **separadas tus cuentas** de email personal y profesional

¡Búscate en internet! Todo contenido que aparezca sobre ti y no esté bajo tu control puede considerarse un riesgo

Antes de instalar cualquier aplicación, **revisa sus políticas de privacidad**.

LOS DATOS BIOMÉTRICOS: LAS HUELLAS DACTILARES

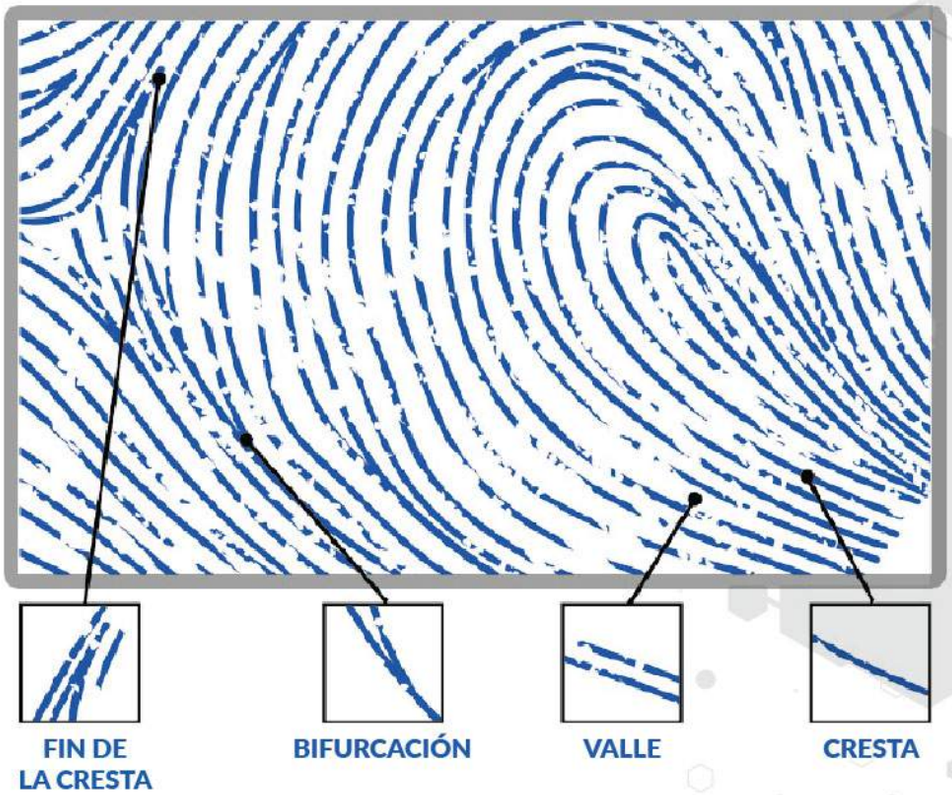
2A. PARTE

Los **sistemas biométricos de reconocimiento de huellas dactilares** son los más comúnmente utilizados debido a lo fácil que resulta recolectar de las personas este dato.

Las huellas dactilares se forman a partir de la superficie desigual de la piel de los dedos de la mano, en donde se identifican diversas protuberancias y hendiduras conocidas como **crestas y valles**, las cuales se encuentran dispuestas de modo único.

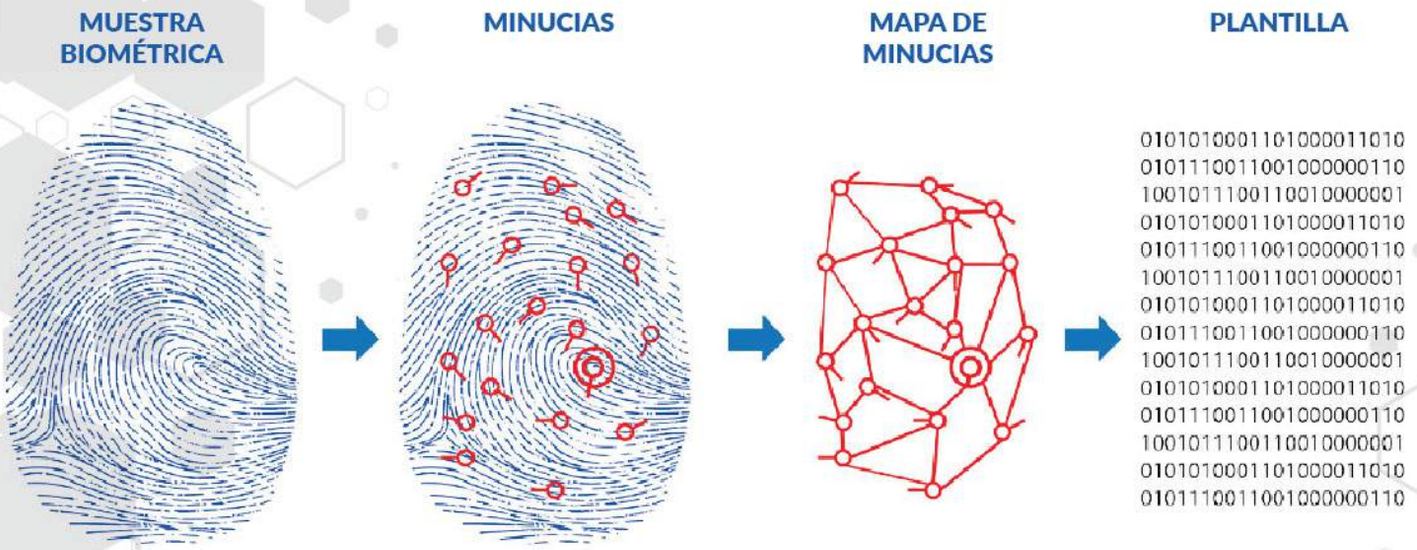
Si bien a una huella dactilar se le pueden aplicar procedimientos manuales de reconocimiento biométrico conocidos como técnica biométrica de correlación, la presente guía **se enfocará a la técnica biométrica automatizada basada en minucias**.

Cuando se registra una huella dactilar en un sistema de reconocimiento, ésta aparece como una serie de líneas oscuras que representan las crestas y de líneas blancas que representan los valles, ubicados entre las crestas. A menudo, las crestas son más cortas y se detienen y comienzan abruptamente. Esta combinación de crestas y valles, con sus correspondientes ubicaciones, direcciones, bifurcaciones, inicios y finales -las minucias-, resultan en un patrón único de características de cada huella dactilar. Las minucias son, entonces, aquellos **puntos de interés en toda huella digital**.



Fuente:
GAO adaptación de datos del FBI

La información de las minucias -principalmente las bifurcaciones y las terminaciones de las crestas, aunque también se utilizan otras minucias- es la que se recolecta y la que posteriormente se utiliza para desarrollar la plantilla.



Uno de los componentes esenciales en el campo del reconocimiento de huellas dactilares, es el desarrollo de **estándares técnicos**. Este enfoque es manejado por la vasta variedad de algoritmos y sensores disponibles en el mercado.

La interoperabilidad está relacionada con los estándares de la tecnología y es otro aspecto crucial en la implementación del producto.

Las **plantillas** generadas por un sistema biométrico para reconocimiento dactilar deberían ser capaces de ser interpretadas por otra computadora usando un sistema diferente.

Cabe señalar que, de acuerdo con el análisis de los sistemas biométricos para reconocimiento dactilar, realizado por **NIST,7** derivado de la **USA PATRIOT ACT**, en donde se evaluó la precisión de distintos sistemas de esta clase, se concluyó que la utilización de cuatro a diez huellas dactilares resulta tan eficiente como la utilización de una sola huella dactilar de alta calidad

Fuente:

- *Guía para el Tratamiento de Datos Biométricos*, Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)

EL FENÓMENO FINTECH LLEGÓ PARA QUEDARSE

Por: Héctor Ortega
CEO de Beernnovation

En el año 2002 hubo una noticia importante para el sector financiero, la **Secretaría de Hacienda y Crédito Público** otorgó una licencia bancaria a **Banco Azteca**, un evento que no ocurría desde hace muchos años en México y la oferta que atendía era a un segmento de la base de la pirámide.

Quién hubiera imaginado que 20 años después estaríamos frente a una revolución en nuestro ecosistema financiero, y es importante tener en cuenta estos dos conceptos: **"Revolución" y "Ecosistema"**.

Hoy se contempla ingresar de manera mucho más simple al sector financiero, el regulador reconoce y está abierto a escuchar nuevos modelos, ha evolucionado para atender a las nuevas demandas del mercado, lo que ha generado una revolución en dicho sector.

La revolución empieza con la Ley Fintech como un parteaguas, sitúa a México con los grandes jugadores a nivel mundial, pues reconoce y atiende a un mercado demandante y muy grande, donde las oportunidades y nuevos modelos de negocio encuentran muy buena acogida.

El ecosistema se formará por el mandato de *Open Banking*, integrando a todos los actores bajo un sólo concepto para generar colaboración entre ellos, y con terceros a fin de generar nuevos negocios y favorecer la inclusión financiera.

Existen muchas más aristas de **Ley Fintech**, aunque lo que revoluciona el ecosistema es **Open Banking, donde el cliente es dueño de su información y puede compartirla con quién decida, derrumbando una vieja práctica que durante años fue muy común, el llamado "secreto bancario".**

Open Banking se habilita por medio de *APIS* (Interfaz de Programación de Aplicaciones, por sus siglas en inglés) que es una manera de ofrecer información o datos entre aplicaciones. Para comprender mejor este aspecto, pensemos en Twitter. Para ver los mensajes en esta red social se utiliza una aplicación o el sitio web de la misma, pero si quisiéramos cambiarle los colores o presentarlo de otra manera, entonces necesitamos únicamente la información. Este módulo de software que entrega sólo información y datos, se denomina *API* y sirve para intercambiar procesos entre aplicaciones.

Open Banking incluye a todos y cada uno de los actores del ecosistema, y al ser tema mandatorio por el regulador, esperamos tener muchos procesos que compartan información de los clientes (*API*), si bien falta mucho camino por recorrer, ya se tiene una base sólida y se realizan esfuerzos importantes para lograr un consenso de qué información se debe publicar, bajo qué esquema de seguridad y mecanismos de control para los clientes. No es menester de este artículo profundizar en el esquema técnico, el objetivo es dar una visión del impacto que representa para el ecosistema.

Al estar todos obligados a participar, se requiere una avanzada tecnológica importante, si la transformación digital en algunas organizaciones no estaba dentro de los proyectos a realizar, por normativa tendrán que realizarlo y de una manera importante, es pues el primer reto significativo para la industria.

Este hito dentro de la industria viene no sólo a habilitar nuevos negocios, genera retos a las entidades financieras que superan el aspecto tecnológico y pasan al de negocio digital, donde lo que importa es la disponibilidad de las plataformas, para un cliente cada vez más exigente.

*A manera de conclusión, me parece que la primera parte del proceso de **Open Banking**, empieza en conocer a qué se refiere y hasta dónde se debe implementar, pensando en como generar valor para la organización y sus clientes. Es un tema normativo pero de fondo es innovación para todos los servicios financieros, es momento de subirse en la transformación digital o alguien más lo hará por nosotros, para competir con mejores productos, procesos, herramientas para un consumidor cada vez más acostumbrado a la **inmediatez y a la experiencia digital**.*

CALENDARIO DE CURSOS 2019

AGOSTO	AGOSTO	AGOSTO
Fintech, regulación, cumplimiento y tecnología.	*Banking as a Service.*	La Biometria en la Regulación Bancaria.
SEPTIEMBRE	**SEPTIEMBRE**	**SEPTIEMBRE**
Creación de Productos Digitales Financieros.	La Biometria en la Regulación Bancaria.	Ciberseguridad.
OCTUBRE	**OCTUBRE**	**OCTUBRE**
Marco Legal en Fintech.	La Biometria en la Regulación Bancaria.	Protocolo para Atención de Asuntos por posible Robo de Identidad.
NOVIEMBRE	**NOVIEMBRE**	**NOVIEMBRE**
Previsiones Legales en torno al Robo de Identidad en México: Protección de Datos Personales y Seguridad de la Información.	Esquema Legal del Robo de Identidad en México.	La Biometria en la Regulación Bancaria.

Fechas, sedes y horarios por confirmar.

Para mayores informes, puede registrarse en:

robodeidentidad.mx/cursos

o bien, escribirnos a

ventas@robodeidentidad.mx

COMUNICADO:
COMITÉ DE CRÉDITO EN LÍNEA

Con el fin de fomentar el crédito responsable, seguro y legal en el mercado del financiamiento personal a través de herramientas, aplicaciones y plataformas de internet, la **Asociación Mexicana de Entidades Financieras Especializadas (AMFE)** constituyó el **Comité de Crédito en Línea**.

Se eligió como vicepresidente de este sector a **Adalberto Flores Ochoa, CEO de Kueski**, quien junto con los representantes de otras empresas como **Konfío, Moneyman, Vivus y Ferratum**, darán prioridad a programas de autorregulación y de asistencia y educación financiera al público.

Estas firmas se definen como complementos de la banca comercial para dispersar el crédito a personas y familias que requieren una atención especializada, así como para apoyar a aquellos que afrontan una emergencia, promoviendo la generación de un historial crediticio saludable en torno a los marcos legales que permiten la inclusión financiera en México.

Contacto:
Monserrat Villeda | AMFE A.C.
mvilleda@amfe.com.mx

AMFE
Asociación Mexicana de Entidades Financieras Especializadas

partner de: PIMA

Robo de IDentidad MX

REVISTA DIGITAL

www.robodeidentidad.mx

ventas@robodeidentidad.mx

robodeientidadmx

Revista Digital Robo de IDentidad MX

Heriberto Frías 1145, Col. del Valle Centro, 03100, Ciudad de México

Tels: (55) 9185-6835 y (55) 5434-4438. Email: revista@robodeidentidad.mx